Remarks and Arguments

Applicants have carefully considered the Office Action dated June 18, 2003 and the references cited therein. Applicants respectfully request reexamination and reconsideration of the application.

Claim 11 has been amended for grammatical purposes. This amendment has not been made to distinguish over any reference of record or for patentability purposes to comply with 35 USC 112. Accordingly, no narrowing of any corresponding equivalents to which this claim is entitled is intended by this amendment.

Claims 1-12 and 14-18 stand rejected under 35 USC Section 102(b) as being anticipated by US Patent 5,552,897, Mandelbaum et al., hereafter "Mandelbaum". In setting forth the rejections of claims 1 and 7, the Examiner alleges that Mandelbaum discloses a method and apparatus which includes substantially all of the limitations of each of the respective claims. Prior to addressing the Examiner's rejections, Applicants ask that the Examiner consider the following. As set forth in the Background of the Invention section of subject application, the present invention addresses the need to provide electronic mail capabilities to an off-line user who is operating with an abbreviated address book. In order to use select functions of an electronic mail system, a copy of a public address book must also be placed on the remote computer. However, in large enterprises, several different public address books may exist. If all of these are combined, to form one large address book the overall size would generally be too large for most remote computers, such as laptop computers. Therefore, the various public address books are compressed or abbreviated by means of a program called an "aggregator" which generates an abbreviated address book called a "directory catalog" which contains some of the information of the public address books, but is much smaller in size. The digital certificates which are used to encrypt e-mail are typically 1K-2K bytes in length, but may be up to 20K bytes in length. Because of this significant length, they are typically *not included in the directory catalog*. Therefore, if a user operating remotely and "off-line" attempts to send e-mail to a recipient where the e-mail must be encrypted, the digital certificate will not be available.

According to the inventive technique disclosed in the subject application, when mail is to be sent by an off-line user to a recipient who holds a digital certificate, the sender's electronic mail program allows the sender to compose the mail, but the mail is placed in plain text in the sender's local outbox and flagged for subsequent encryption. When the sender later connects to a mail server to send the outgoing mail, *the sender's mail software will request the recipient's certificate from the server and use the received certificate to encrypt the mail message before it leaves the sender's workstation.* As such, *the digital certificate used to encrypt the message is not contained on the user's system at the time the message is composed.*

Conversely, the system disclosed in Mandelbaum is similar to the systems described as problematic in the subject application. In Mandelbaum, the public encryption keys are maintained in recipient list, Table 401. It is this very type of large tabular data structure similar to that disclosed in Mandelbaum, which the subject invention is designed to avoid.

After reviewing the portions of the Mandelbaum reference provided, Applicants respectfully traverse the rejection as improper. Specifically, to anticipate a claim, a reference must teach every element of the claim (MPEP Section 2131). A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. Claim 1 recites a method for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a digital certificate including the limitation of "(c) *when the sender is on-line, in response to the flag, requesting the digital certificate from the mail system*" (claim 1, lines 7-8). Such limitation is disclosed in the subject specification (page 9, lines 4-29; page 10, line 16-28; Figs. 4 and 6). The Examiner has failed to indicate where Mandelbaum discloses the limitation of "*requesting the digital certificate from the mail system* ". The system disclosed in Mandelbaum is directed to a facsimile apparatus 100 that interacts with a remote smart card 175 on which a plurality of public and private encryption keys are stored (Mandelbaum, Figure 5). As such, Mandelbaum discloses a system in which a remote recipient utilizes encryption keys stored in the local remote apparatus (the smart card 175) to access and decrypt facsimile messages. Conversely, the present

invention discloses a system and techniques in which the author of an electronic mail message composes the message remotely or off line and then requests that the electronic mail application retrieve, from a remote public address book, the encryption key required to encrypt the message. The two respective processes are distinctly different. In one, a recipient maintains the decryption keys in order to remotely receive messages. In the other, a sender requests a remotely stored encryption certificate to encrypt a message prior to sending thereof. The sections of the Mandelbaum reference cited by the Examiner do not disclose techniques or mechanisms for *requesting a digital certificate from the mail system* following the message composition and prior to its transmission, as in the present invention.

Accordingly, Applicants respectfully assert that claim 1, as filed, is not anticipated by Mandelbaum. Claims 2-6 include all the limitations of claim 1 and are likewise believed not anticipated by Mandelbaum for at least the same reasons as claim 1, as well as for the merits of their own respective limitations.

Applicants respectfully traverse the rejection of claims 14-18 under 35 USC Section 102(b) as improper. Specifically, claims 14-18 include all the limitations of independent claim 13, and, therefore, are more narrow in scope than independent claim 13 from which they depend. Yet claim 13 has been rejected as obvious in light of the combined teachings of Mandelbaum and Baltzley. In setting forth the rejection of claim 13, the Examiner admits that Mandelbaum does not explicitly disclose a computer program product used for encrypting electronic message is composed by a sender for delivery over a mail system to a recipient who holds a digital certificate. However, claims 14-18 each explicitly recite a computer program product. Accordingly, Applicants are puzzled how dependent claims 14-18 may be anticipated by Mandelbaum in light of the Examiner's express admission in the deficiency of Mandelbaum's teachings regarding a computer program product. In light of the foregoing, Applicants submit no further arguments or traversals, at this time, regarding the rejection of claims 14-18, until the Examiner clarifies the rejections thereof.

Claim 7 includes language similar to that contained within claim 1. Claim 7 recites an apparatus for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a

digital certificate including "a verification mechanism which is operable when the sender is on-line and, in response to the flag, *requests the digital certificate from the mail system* " (claim 7, lines 8-9). The Examiner has not shown where Mandelbaum discloses a *verification mechanism that requests the digital certificate from the mail system* itself. Accordingly, Applicants respectfully assert that claim 7 is not anticipated by Mandelbaum for at least the same reasons as set forth above with respect to the traversal of the claim 1 rejections, as well as for the merits of its own respective limitations. Claims 8-12 include all the limitations of claim 7 and are likewise believed not anticipated by Mandelbaum for at least the same reasons as claim 7, as well as for the merits of their own respective limitations.

Claims 13, 19 and 20 stand rejected under 35 USC Section 103(a) as being anticipated by Mandelbaum in view of US Patent 6, 292, 895, hereafter referred to as "Baltzley". In setting forth the rejection of claims 13, 19 and 20, the Examiner admits that Mandelbaum does not explicitly disclose a computer program product used for encrypting electronic message is composed by a sender for delivery over a mail system to a recipient who holds a digital certificate. Instead, the Examiner is relying on Baltzley to disclose such teaching, alleging that Balsley discloses a user computer program which generates a user identifier, private key, public-key, and a user pass phrase.

Applicants traverses the rejection of claims 13 and 19 under 35 U.S.C. §103(a) on the grounds that the Examiner has failed to create a *prima facie* case of obviousness. In accordance with MPEP §2143.03, to establish a *prima facie* case of obviousness 1) the prior art reference (or references when combined) must teach or suggest *all* of the claim limitations; 2) there must be some suggestion or motivation to modify a reference or combine references; and 3) there must be a reasonable vexpectation of success.

By the own Examiner's admissions of record and for the same reasons as set forth above with respect to the traversal of the claim 1 rejections, Applicants respectfully assert that Mandelbaum does not disclose the subject matter of claims 13 and 19. Specifically, claim 13 is directed to a computer program product for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system and specifically recites "program code operable when the

sender is on-line and, in response to the flag, for requesting the digital certificate from the mail system" (claim 13, lines 9-10). Claim 19 is the computer and data signal counterparts to claim 13 and recites similar language (claim 19, lines 8-9). Baltzley does not teach disclose or suggest the teachings absent from Mandelbaum. Specifically, in Baltzley, once a digital message is generated, it is encrypted with a client recipient's public key. The encrypted message is then transmitted to the client recipient's computer (Baltzley, column 2, lines 55-57). As such, the system disclosed therein does not provide a teaching suggestion or disclosure of *program code for requesting the digital certificate from the mail system*, as recited in claims 13 and 19. The Examiner's statements regarding the motivation for combining the Mandelbaum and Baltzley references are irrelevant in the absence of any teaching or disclosures to support such assertions. Accordingly, Applicants respectfully assert that claims 13 and 19 are believed patentable over the combination of Mandelbaum and Baltzley whether considered singularly or in combination.

Claims 14-18 include all the limitations of claim 13 and are likewise believed allowable over the combination of Mandelbaum and Baltzley for at least the same reasons as claim 13, as well as for the merits of their own respective limitations. Similarly, claim 20 includes all the limitations of claim 19 and is likewise believed allowable over the combination of Mandelbaum and Baltzley for at least the same reasons as claim 19, as well as for the merits of its own respective limitations.

Applicants believe the claims are in allowable condition. A notice of allowance for this application is solicited earnestly. If the Examiner has any further questions regarding this amendment, he/she is invited to call Applicants' attorney at the number listed below. The Examiner is hereby authorized to charge any fees or credit any balances under 37 CFR §1.17, and 1.16 to Deposit Account No. DA-12-2158.

Respectfully submitted,

Bruce D. Jobse Date: 9/16/03

Bruce D. Jobse, Esq. Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656